

A LOCAL TO GLOBAL PRINCIPLE FOR DENSITIES OVER FUNCTION FIELDS

GIACOMO MICHELI

ABSTRACT. Let d be a positive integer and \mathbb{H} be an integrally closed subring of a global function field F . The purpose of this paper is to provide a general sieve method to compute densities of subsets of \mathbb{H}^d defined by local conditions. The main advantage of the method relies on the fact that one can use results from measure theory to extract density results over \mathbb{H}^d . Using this method we are able to compute the density of the set of polynomials with coefficients in \mathbb{H} which give rise to “good” totally ramified extensions of the global function field F . As another application, we give a closed expression for the density of rectangular unimodular matrices with coefficients in \mathbb{H} in terms of the L -polynomial of the function field.

1. INTRODUCTION

In [1, Lemma 20] B. Poonen and M. Stoll formalise a nice sieve method for computing densities using p -adic analysis. Essentially, the method consists of writing a given set $U \subseteq \mathbb{Z}^d$ in terms of local conditions at the completions of \mathbb{Q} ; once this is done, the density of U can be computed by determining the measures of certain sets $U_p \subseteq \mathbb{Z}_p$ which are associated to the local conditions which define U . It is worth mentioning that the result is a powerful evolution of Ekedhal’s Sieve (See [2]).

In this paper we present the extension of this method to global function fields i.e. univariate function fields over finite fields. Let \mathbb{H} be a non-trivial integrally closed subring of a function field F and \mathcal{S} be the set of places of F where all the functions in \mathbb{H} are well defined. It is well known (see for example [13, Theorem 3.2.6]) that \mathbb{H} consists exactly of the intersection of all the valuation rings \mathcal{O}_P of F for $P \in \mathcal{S}$. Vice versa, it also holds that an arbitrary intersection of valuation rings of F is an integrally closed subring [13, Proposition 3.2.5]). We will be interested in computing the density of a subset U of \mathbb{H}^d .

Key words and phrases. Function fields; density; local to global principles; totally ramified places; rectangular unimodular matrices.

Before doing so, we first need to specify what we mean by “density” of U in the function field context. Over the set of rational integers \mathbb{Z} , the density of a subset $U \subseteq \mathbb{Z}^d$ is computed by considering the sequence of ratios between the number of points of U falling in the hypercube of side $2B$ and centred at the origin, and $(2B)^d$. If $\{a_B\}_{B \in \mathbb{N}}$ is this sequence of ratios and u is its limit (if exists), then we say that U has density u . In the case of \mathbb{H}^d , we explain how to use Moore-Smith convergence [3, Chapter 2] to define a notion of limit over the directed set of positive divisors having support in the complement of \mathcal{S} (see also [4]). Once this is understood, Riemann-Roch spaces of positive divisors having support in the complement of \mathcal{S} will play the role of intervals, and therefore products of such spaces will play the role of hypercubes.

Let $D_{\mathcal{S}}$ be the set of positive divisors having support in the complement of \mathcal{S} . The striking analogy between \mathbb{Z} and \mathbb{H} which allows our density definition (see Subsection 1.1) is given by

$$\mathbb{Z} = \bigcup_{B \in \mathbb{N}} [-B, B[\cap \mathbb{Z} \quad \text{and} \quad \mathbb{H} = \bigcup_{D \in D_{\mathcal{S}}} \mathcal{L}(D).$$

In particular the reader should notice that the definition of density we will provide is consistent with the one used in the literature in the case of $\mathbb{F}_q[x]$: if $F = \mathbb{F}_q(x)$, $\mathbb{H} = \mathbb{F}_q[x]$ and P_{∞} is the place at plus infinity with respect to x , we have that $D_{\mathcal{S}} = \{nP_{\infty}\}_{n \in \mathbb{N}}$ and therefore

$$\mathcal{L}(D) = \mathcal{L}(nP_{\infty}) = \{f \in \mathbb{F}_q[x] : \deg(f) \leq n\},$$

which induces the natural definition of density in the context of $\mathbb{F}_q[x]$.

The essence of the presented method (Theorem 2.1) is to polarize the difficulty of the problem: in fact, on one hand the p -adic formalism allows to easily compute a “candidate” for the density of a certain subset of \mathbb{H}^d by using tools from measure theory, on the other hand all the difficulty of the problem is unloaded on proving that the limit of a certain sequence (given by Equation (2.1)) tends to zero. In particular, we show that whenever the local conditions are actually related in a certain way to polynomial equations, the limit can be proven to be always zero (Theorem 2.2).

The entire machinery we build in Section 2 is then used to produce two new results in Sections 3 and 4.

In Section 3 we compute the probability that a “random” polynomial f of fixed degree with coefficient in an given integrally closed subring $\mathbb{H} \subset F$ gives rise to a totally ramified extension $E = F[y]/(f(y))$ of F for which the equation $f(y) = 0$ is “good enough” around the totally ramified place (in terms of Definition 3.1).

Let k, m be positive integers such that $k < m$ and R be a domain. The question whether a homomorphism of R^k in R^m can be extended to an automorphism of R^m raised many interesting questions in the past (see for instance Serre's Conjecture, which is proven in [5, 6]). In Section 4 we close the problem of computing the density of homomorphisms of \mathbb{H}^k in \mathbb{H}^m which can be extended to automorphisms of \mathbb{H}^m . In the case of $\mathbb{H} = \mathbb{F}_q[x]$, these homomorphisms arise from context of convolutional codes (see for example [7] or [8]) and their density was studied in [9] and [10]. In Theorem 4.4 we show that the density of unimodular matrices over \mathbb{H} is a rational number and can be explicitly computed as soon as the complement of the holomorphy set \mathcal{S} is finite.

1.1. Preliminary definitions and notations. Let \mathbb{F}_q be a finite field. In this paper all the function fields are global and have full constant field \mathbb{F}_q . We denote by \mathcal{O}_P a valuation ring of function field F , having maximal ideal P . The set of all the places of F will be denoted by \mathbb{P}_F . If \mathcal{S} is a proper subset of \mathbb{P}_F , we denote by \mathcal{S}_t the subset of places of \mathcal{S} of degree greater than t . Moreover, we write $\mathbb{H}_{\mathcal{S}}$ to denote the *holomorphy ring* of \mathcal{S} i.e. the intersection of all the valuation rings associated to the places of \mathcal{S} :

$$\mathbb{H}_{\mathcal{S}} = \bigcap_{P \in \mathcal{S}} \mathcal{O}_P.$$

Sometimes, we will refer to \mathcal{S} as the *holomorphy set* of $\mathbb{H}_{\mathcal{S}}$ and to $\mathbb{H}_{\mathcal{S}}$ as the *holomorphy ring* of \mathcal{S} . Holomorphy rings are integrally closed in F and any integrally closed subring of F is an holomorphy ring [13, Proposition 3.2.5, Theorem 3.2.6]. In the whole paper we consider only holomorphy rings whose holomorphy set has finite complement in the set of all places of F . The most immediate example of holomorphy ring is $\mathbb{F}_q[x]$ as this consists of the intersection of all the valuation rings of $\mathbb{F}_q(x)$ different from the valuation ring at infinity.

Let $\text{Div}(F)$ be the set of divisors of F i.e. the free abelian group having as base symbols the elements in the set \mathbb{P}_F . For $D = \sum_{P \in \mathbb{P}_F} n_P P \in \text{Div}(F)$, we denote by $\text{supp}(D)$ the finite subset of \mathbb{P}_F for which n_P is non-zero. Moreover, we will write $D \geq 0$ whenever $n_P \geq 0$ for any P in \mathbb{P}_F . Let

$$\text{Div}^+(F) = \{D \in \text{Div}(F) \mid D \geq 0\}$$

Let $\mathcal{D}_{\mathcal{S}}$ be the subset of divisors of $\text{Div}^+(F)$ having support over the complement of \mathcal{S} in \mathbb{P}_F . As $\mathcal{D}_{\mathcal{S}}$ is a directed set, we can define via Moore-Smith Convergence (see [3, Chapter 2] and more specifically for this context [11]) a notion of limit over $\mathcal{D}_{\mathcal{S}}$. In

this context, we can give an upper density definition for a subset A of \mathbb{H}_S^d as follows:

$$\overline{\mathbb{D}}_S(A) := \limsup_{D \in \mathcal{D}_S} \frac{|A \cap \mathcal{L}(D)^d|}{q^{\ell(D)d}}$$

where $\mathcal{L}(D)$ is the Riemann-Roch space attached to the divisor D and $\ell(D) = \dim_{\mathbb{F}_q}(\mathcal{L}(D))$. Analogously, one can give a notion of lower density $\underline{\mathbb{D}}_S$ by considering the inferior limit of the sequence. Whenever these two quantities are equal, we say that a subset A of \mathbb{H}_S^d has a well-defined density $\overline{\mathbb{D}}_S(A) = \underline{\mathbb{D}}_S(A) = \mathbb{D}_S(A)$.

For a valuation ring \mathcal{O}_P let us denote by $\widehat{\mathcal{O}}_P$ the completion of \mathcal{O}_P with respect to the P -adic metric. In addition, let us denote by μ_P the normalized Haar measure on $\widehat{\mathcal{O}}_P$ with respect to the P -adic metric. For a subset $U \subseteq \widehat{\mathcal{O}}_P$ we denote by ∂U the boundary of U with respect to the topology induced by the P -adic metric. For a multivariate polynomial $f \in F[x_1, \dots, x_n]$, we will denote by $\deg_{x_i}(f)$ (resp. $\deg_{\text{hom}}(f)$) the degree of f in the variable x_i (resp. the degree of the homogenization of f). Whenever f has all the coefficients in a given valuation ring \mathcal{O}_P , we will denote by $\deg_{x_i}^P(f)$ (resp. $\deg_{\text{hom}}^P(f)$) the degree of f in the variable x_i (resp. the degree of the homogenization of f) in $(\mathcal{O}_P/P)[x_1, \dots, x_n]$. For a positive integer n and a given commutative domain R , we will denote by $\text{GL}_n(R)$ the set of $n \times n$ matrices whose determinant is a unit of R .

2. THE LOCAL TO GLOBAL PRINCIPLE FOR DENSITIES OVER GLOBAL FUNCTION FIELDS

In this section we describe the local to global principle which will be used later on. This result is the function field analogue of [1, Lemma 20].

Theorem 2.1. *Let d be a positive integer, \mathcal{S} be a subset of places of F and \mathbb{H}_S the holomorphy ring of \mathcal{S} . For any $P \in \mathcal{S}$, let $U_P \subseteq \widehat{\mathcal{O}}_P^d$ be a measurable set such that $\mu_P(\partial U_P) = 0$. Suppose that*

$$(2.1) \quad \lim_{t \rightarrow \infty} \overline{\mathbb{D}}_S(\{a \in \mathbb{H}_S^d \mid a \in U_P \text{ for some } P \in \mathcal{S}_t\}) = 0.$$

Let $\pi : \mathbb{H}_S^d \rightarrow 2^{\mathcal{S}}$ defined by $\pi(a) = \{P \in \mathcal{S} : a \in U_P\} \in 2^{\mathcal{S}}$. Then

- (i) $\sum_{P \in \mathcal{S}} \mu_P(U_P)$ is convergent.
- (ii) Let $\Gamma \subseteq 2^{\mathcal{S}}$. Then $\nu(\Gamma) := \mathbb{D}_S(\pi^{-1}(\Gamma))$ exists and ν defines a measure on $2^{\mathcal{S}}$.

- (iii) ν is concentrated at finite subsets of \mathcal{S} . In addition, if $T \subseteq \mathcal{S}$ is finite we have:

$$\nu(\{T\}) = \left(\prod_{P \in T} \mu_P(U_P) \right) \prod_{P \in \mathcal{S} \setminus T} (1 - \mu_P(U_P)).$$

Proof. Throughout the proof \mathcal{S} will be fixed, so we will denote $\mathbb{H}_{\mathcal{S}}$ by \mathbb{H} . What we need to do is to translate the proof of [12] to the context of function fields. Essentially, we need to understand how the measure of P -adic intervals can be translated into density via the use of Riemann-Roch Theorem [13, Theorem 1.5.15]. Once this is done, the same arguments of the proof of [1, Lemma 20] will apply to this context. We define a P -interval in $\widehat{\mathcal{O}}_P$ as the set $\{x \in \widehat{\mathcal{O}}_P : x \equiv a \pmod{P^{e_P}}\}$ for some $e_P \in \mathbb{N}$ and $a \in \widehat{\mathcal{O}}_P$. A P -box I_P will just be a product of P -intervals:

$$I_P = \{x \in \widehat{\mathcal{O}}_P^d : x_j \equiv a_j \pmod{P^{e_{P,j}}} \text{ for } j \in \{1, \dots, d\}\}.$$

To simplify notation, we say that a P -box is a P -cube if it has the form

$$C_P = \{x \in \widehat{\mathcal{O}}_P^d : x_i \equiv y_i \pmod{P^{e_P}}, i \in \{1, \dots, d\}\}$$

for some $e_P \in \mathbb{N}$ and $(y_1, \dots, y_d) \in \widehat{\mathcal{O}}_P^d$. In other words, C_P is the cartesian product of intervals of equal length. We say that $c_P = (y_1, \dots, y_d)$ is the *center* of the cube. Let A be a finite subset of \mathcal{S} . Let us now compute the density of the elements in \mathbb{H}^d which are mapped in a product of a finite number of P -boxes via the natural embedding $\mathbb{H}^d \rightarrow \prod_{P \in A} \widehat{\mathcal{O}}_P^d$. Let $I = \prod_{P \in A} I_P$ be such product of P -boxes. For any P , the P -box I_P can be covered with a finite number l_P of disjoint cubes of equal size e_P , as all the congruences can be decomposed in terms of the finest congruence, given by $\max\{e_{P,j} : j \in \{1, \dots, d\}\} =: e_P$. Therefore, one can write

$$I = \prod_{P \in A} I_P = \prod_{P \in A} \bigsqcup_{i=1}^{l_P} C_P^{(i)}$$

with $\mu_P(C_P^{(i)}) = q^{-d \deg(P) e_P}$ independently of i .

We consider the diagram

$$\begin{array}{ccc} \mathbb{H}^d & \xrightarrow{\iota} & \prod_{P \in A} \widehat{\mathcal{O}}_P^d \supseteq I \\ \downarrow \pi_J & & \downarrow \pi'_J \\ (\mathbb{H}/J)^d & \xrightarrow{\psi} & \prod_{P \in A} (\widehat{\mathcal{O}}_P / P^{e_P})^d =: R \end{array}$$

where $J = \prod_{P \in A} P^{e_P} \subseteq \mathbb{H}$, the map ι is the natural inclusion, and ψ is the isomorphism (coming from the Chinese Remainder Theorem) which makes the diagram

commutative. On the right-hand side, we can immediately compute the product measure m of I by looking at its definition, getting $m = \prod_{P \in A} l_P q^{-d \deg(P) e_P}$. It remains to show that the density of $\iota^{-1}(I)$ is indeed m . For this, let us decompose I . Let \mathcal{I}_P be a finite set indexing the cubes which cover I_P and let $\mathcal{I} = \prod_{P \in A} \mathcal{I}_P$. Any given $i = (i_P)_{P \in A} \in \mathcal{I}$ determines a choice of cubes as follows: for each place $P \in A$ we select exactly one cube $C_P^{(i_P)}$, having center $c_P^{(i_P)}$. We now build a C_i as the product $\prod_{P \in A} C_P^{(i_P)}$. Clearly, the set of C_i 's built in this way has cardinality $\prod_{P \in A} l_P$ and covers I via a disjoint union. If we can now prove that the density of $\iota^{-1}(C_i)$ is independent of the choice of $i \in \mathcal{I}$, then we will have that

$$(2.2) \quad \mathbb{D}(\iota^{-1}(I)) = \mathbb{D}(\iota^{-1}(C_i)) \cdot \prod_{P \in A} l_P.$$

To achieve this, we now explicitly compute the value $\mathbb{D}(\iota^{-1}(C_i))$. As the diagram above is commutative, we can equivalently compute the density of elements of \mathbb{H}^d falling into $\psi^{-1}\pi'_J(C_i)$ via the map π_J . Let $z_{C_i} \in \pi_J^{-1}\psi^{-1}\pi'_J((c_P^{(i)})_{P \in A})$. Notice that we have

$$\iota^{-1}(C_i) = \pi_J^{-1}\psi^{-1}\pi'_J(C_i) = z_{C_i} + J\mathbb{H}.$$

Observe that for any divisor $D \in \mathcal{D}_S$, the map π_J restricted to $\mathcal{L}(D)$ is \mathbb{F}_q -linear. Let g be the genus of F . Therefore if we denote by $z_{C_i, j}$ the j -th component of z_{C_i} , we have

$$|\mathcal{L}(D) \cap (z_{C_i, j} + J\mathbb{H})| = |\mathcal{L}(D) \cap J\mathbb{H}| = \left| \mathcal{L} \left(D - \sum_{P \in A} e_P P \right) \right| = q^{\ell(D - \sum_{P \in A} e_P P)},$$

which for D of large degree, equals $q^{\deg(D - \sum_{P \in A} e_P P) + 1 - g}$ by Riemann-Roch Theorem. We can finally compute the density of elements mapping in the cube C_i (which is in fact independent of i , as we wanted):

$$\begin{aligned} \mathbb{D}(\iota^{-1}(C_i)) &= \lim_{D \in \mathcal{D}_S} \frac{|\mathcal{L}(D)^d \cap \pi_J^{-1}\psi^{-1}\pi'_J(C_i)|}{q^{\ell(D)d}} \\ &= q^{-\ell(D)d} \prod_{j=1}^d |\mathcal{L}(D) \cap (z_{C_i, j} + J\mathbb{H})| = q^{-(\sum_{P \in S_t} e_P \deg(P))d}. \end{aligned}$$

Using now Equation (2.2) we get the final claim by comparing m with $\mathbb{D}(\iota^{-1}(I))$. Since now we have proved the theorem for boxes, all the arguments of the proof of [1, Lemma 20] are now straightforward to apply. In fact, suppose for a moment that the set of P 's in \mathcal{S} for which U_P is different from the empty set is a finite set A . Now, let T be a finite set of places. Assuming that $\mu_P(\partial U_P) = 0$, one can cover each of the U_P 's from the interior (resp. U_P^c) with a finite set of boxes which well approximate

the measure $\mu_P(U_P)$ (resp. $\mu_P(U_P^c)$). In particular one has

$$\nu(\{T\}) \geq \left(\prod_{P \in T} \mu_P(U'_P) \right) \prod_{P \in \mathcal{S} \setminus T} (1 - \mu_P(U'_P)),$$

where the products above are both finite and U'_P union of the boxes for each P , where the theorem holds. As we can apply the symmetric argument with a set of external approximations U''_P we have

$$\nu(\{T\}) \leq \left(\prod_{P \in T} \mu_P(U''_P) \right) \prod_{P \in \mathcal{S} \setminus T} (1 - \mu_P(U''_P)),$$

from which the claim follows by letting the approximation get sharper and then $\mu_P(U''_P)$ and $\mu_P(U'_P)$ tend to $\mu(U_P)$.

On the other hand, if A is an infinite set, one easily sees that an approximation with finitely many U_P is good enough, as long as condition (2.1) is verified. To see this, let T be a finite subset of \mathcal{S} and let us recall that \mathcal{S}_t is the set of places of \mathcal{S} of degree larger than t and then \mathcal{S}_t^c is the subset of \mathcal{S} consisting of places of degree less than or equal to t . Observe that for a positive integer t such that \mathcal{S}_t^c contains T we can define a partial approximation of $\pi^{-1}(\{T\})$

$$W_t = \{a \in \mathbb{H}_S^d \mid a \in U_P \ \forall P \in T, \ a \notin U_P \ \forall P \in T^c \cap \mathcal{S}_t^c\}.$$

Notice that W_t contains $\pi^{-1}(\{T\})$ so $\mathbb{D}(\pi^{-1}(\{T\})) \leq \mathbb{D}(W_t)$. In addition we have that

$$\mathbb{D}(\pi^{-1}(\{T\})) \geq \mathbb{D}(W_t) - \overline{\mathbb{D}}(W_t \setminus \pi^{-1}(\{T\})).$$

Now, by letting t go to infinity and using condition (2.1) on $\mathbb{D}(W_t \setminus \pi^{-1}(\{T\}))$ one gets the claim. \square

The next Theorem ensures that when the U_P can be expressed in terms of polynomial equations, Condition (2.1) is always verified, similarly to what happens in the case of Ekedhal Sieve for integers [2].

Theorem 2.2. *Let F/\mathbb{F}_q be a global function field and \mathcal{S} be a subset of \mathbb{P}_F with finite complement. Let \mathbb{H}_S be the holomorphy ring of \mathcal{S} . Let $f, g \in \mathbb{H}_S[x_1, \dots, x_d]$ be coprime polynomials. Then*

$$(2.3) \quad \lim_{t \rightarrow \infty} \overline{\mathbb{D}}_S(\{y \in \mathbb{H}_S^d : f(y) \equiv g(y) \equiv 0 \pmod{P} \text{ for some } P \in \mathcal{S}_t\}) = 0.$$

Proof. If $d = 1$ there is nothing to prove so we can suppose $d > 1$. Without loss of generality, we can also suppose $\deg_{x_1}(f) > 0$. Since \mathcal{S} will be fixed throughout

the proof, we will denote $\mathbb{H}_{\mathcal{S}}$ and $\mathbb{D}_{\mathcal{S}}$ by \mathbb{H} and \mathbb{D} respectively. Let us recall that the places in \mathcal{S} are in natural correspondence with the prime ideals of \mathbb{H} , therefore with a small abuse of terminology we will identify this two sets. We first fix t large enough, so that $\deg_{x_1}^P(f) = \deg_{x_1}(f)$ for any P of degree larger than t . Now fix D large enough so that $\deg(D) > t$. Let us also introduce new notation to simplify the computations. For a divisor D , let us define

$$a_t(D) := |\{y \in \mathcal{L}(D)^d : f(y) \equiv g(y) \equiv 0 \pmod{P} \text{ for some } P \in \mathcal{S}_t\}| q^{-d\ell(D)},$$

$$c_P(D) := |\{y \in \mathcal{L}(D)^d : f(y) \equiv g(y) \equiv 0 \pmod{P}\}| q^{-d\ell(D)}.$$

Our first purpose is to estimate $a_t(D)$ for t and D large. First, we notice a simple upper bound for $a_t(D)$:

$$a_t(D) \leq \sum_{P: \deg(P) > t} c_P(D).$$

We now want to estimate the sum above for different regimes of $\deg(P)$ and $\deg(D)$. In order to do so, let us further split the sum as

$$(2.4) \quad \underbrace{\sum_{P: t < \deg(P) \leq \deg(D)} c_P(D)}_{\text{(I)}} + \underbrace{\sum_{P: \deg(P) > \deg(D)} c_P(D)}_{\text{(II)}}.$$

Let us estimate (I). First, we want to give a reasonable estimate for $c_P(D)$ in the specified regime. Notice that for each point of $z \in \mathbb{F}_{q^{\deg(P)}}^d$ satisfying $f(z) \equiv g(z) \equiv 0 \pmod{P}$ there are at most $|\mathcal{L}(D - P)^d|$ preimages of z in $\mathcal{L}(D)^d$, as the evaluation map $\mathcal{L}(D) \rightarrow \mathcal{L}(D)(P) \subseteq \mathbb{F}_{q^{\deg(P)}}$ is linear and has kernel $\mathcal{L}(D - P)$. Let N_P be the number of $\mathbb{F}_{q^{\deg(P)}}$ -points of the variety defined by f and g when reduced modulo P . Let g_F be the genus of F . By observing that $\ell(D) \geq \deg(D) + 1 - g_F$ and that $\ell(D - P) \leq \deg(D) - \deg(P) + 1$ we get:

$$\begin{aligned} c_P(D) &\leq N_P |\mathcal{L}(D - P)|^d q^{-\ell(D)d} \\ &\leq N_P q^{d(\deg(D) - \deg(P) + 1)} q^{-(\deg(D) + 1 - g_F)d} \\ &= N_P q^{(g_F - \deg(P))d}. \end{aligned}$$

As t can be chosen large enough to avoid the places of bad reduction, we can estimate classically N_P as $Cq^{(d-2)\deg(P)}$ for some constant C . It follows that

$$\sum_{P: t < \deg(P) \leq \deg(D)} c_P(D) \leq \sum_{P: t < \deg(P) \leq \deg(D)} \tilde{C} q^{-2\deg(P)}$$

for some other constant \tilde{C} .

Let us estimate (II). Let (f, g) be the ideal generated by f, g in $F[x_1, \dots, x_d]$ and let $J = (f, g) \cap F[x_2, \dots, x_d]$. Since (f, g) has codimension 2, J is principal. Let $h \in F[x_2, \dots, x_d]$ be the generator of J , which can be chosen with coefficients over \mathbb{H} by multiplying by an appropriate element in \mathbb{H} . Let us also assume without loss of generality that $\deg_{x_2}(h) > 0$. Let now D be so large that modulo every prime P of degree larger than $\deg(D)$, we have $\deg_{hom}^P(h) = \deg_{hom}(h)$. Consider now all the elements of $\mathcal{L}(D)^d$ ending with a fixed $r = (r_2, \dots, r_d) \in \mathcal{L}(D)^{d-1}$ and for which $h(r) \neq 0$. Let us estimate their contribution to each $c_P(D)$ in the sum (II). Let I_r be the product of all the prime ideals P of \mathbb{H} such that $\deg(P) > \deg(D)$ and for which there exists $x \in \mathbb{H}$ such that $f(x, r_2, \dots, r_d) \equiv g(x, r_2, \dots, r_d) \equiv 0 \pmod{P}$ (this set is finite as $h(r) \neq 0$). If we denote by u_r the number of distinct primes appearing in the factorization of I_r , the contribution of all the d -tuples ending with r is bounded by $u_r \deg_{x_1}^P(f) = u_r \deg_{x_1}(f)$. By the definition of h , it is clear that $h\mathbb{H}[x_1, \dots, x_d] \subseteq (f, g) \cap \mathbb{H}[x_1, \dots, x_d]$. If we denote by $(f, g)_{I_r}$ the projection of $(f, g) \cap \mathbb{H}[x_1, \dots, x_d]$ in $(\mathbb{H}/I_r)[x_1, \dots, x_d]$, we have that

$$h\mathbb{H}/I_r[x_1, \dots, x_d] \subseteq (f, g)_{I_r}.$$

Therefore this in turn implies that (r_2, \dots, r_d) satisfies $h(r_2, \dots, r_d) \equiv 0 \pmod{I_r}$. Now, the key observation to get the final estimate for (II) is the following: $\deg(D)$ was chosen large in such a way that the homogeneous degree of h is constant modulo P for any P of degree larger than $\deg(D)$. Recall now that every prime ideal P appearing in the factorization of I_r has degree larger than D , therefore

$$u_r \deg(D) < \deg(I_r) \leq \deg(D) \deg_{hom}(h) + C$$

where the constant C depends on the leading coefficients of h (and independent of D), from which it follows that $u_r < \deg_{hom}(h)$, for D large enough.

The reader should now notice that in (II), an element in $\mathcal{L}(D)^d$ ending with r (i.e. of the form (r_1, r)), cannot contribute more than 1 for each $c_P(D)$, as the evaluation map $\mathcal{L}(D) \rightarrow \mathcal{L}(D)(P)$ is an injection to $\mathbb{F}_{q^{\deg(P)}}$. It follows easily that the set of all the d -tuples ending with r contribute at most $u_r \deg_{x_1}(f)$ to the whole sum (II). Now, using the observations above and recalling that we also have to take into account the size of the set T of the $(d-1)$ -tuples $r = (r_2, \dots, r_d)$ such that $h(r) = 0$ for $r \in \mathbb{H}^{d-1}$, we finally get

$$\sum_{P: \deg(P) > \deg(D)} c_P(D) \leq \deg_{x_i}(h) q^{\ell(D)(d-1)} q^{-\ell(D)d} + \sum_{r \in \mathcal{L}(D)^{d-1} \setminus T} q^{-\ell(D)d} u_r \deg_{x_1}(f)$$

$$\leq q^{-\ell(D)}(\deg_{\text{hom}}(h)\deg_{x_1}(f) - 1).$$

At this point we observe that the estimates of (I) and (II) only hold for large values of t and D , so it is now important to notice how the order of the limits in (2.3) is actually taken into account: in order for estimate (I) to hold, it is enough to choose t so large that the primes of bad reduction are avoided. For estimate (II), take D so large that

- its degree is larger than t ,
- the homogeneous degree of h is constant with respect to all places of \mathcal{S} of degree larger than $\deg(D)$,
- the degree of f with respect to x_1 is constant for all places of \mathcal{S} of degree larger than $\deg(D)$.

We can now safely use the two estimates to complete the proof:

$$\begin{aligned} \lim_{t \rightarrow \infty} \lim_{D \rightarrow \infty} a_t(D) &\leq \lim_{t \rightarrow \infty} \lim_{D \rightarrow \infty} \sum_{P: \deg(P) > t} c_P(D) = \\ &\lim_{t \rightarrow \infty} \lim_{D \rightarrow \infty} \sum_{P: \deg(P) > \deg(D)} c_P(D) + \sum_{P: t < \deg(P) \leq \deg(D)} c_P(D) \leq \\ &\lim_{t \rightarrow \infty} \lim_{D \rightarrow \infty} q^{-\ell(D)}(\deg_{\text{hom}}(h)\deg_{x_1}(f) - 1) + \sum_{P: t < \deg(P) \leq \deg(D)} \tilde{C} q^{-2\deg(P)} = \\ &\lim_{t \rightarrow \infty} \sum_{P: t < \deg(P)} \tilde{C} q^{-2\deg(P)}. \end{aligned}$$

This completes the proof, since the sum above is the tail of a subseries of the zeta function of F evaluated at 2, which is converging. \square

The reader should notice that the counting technique using in the estimate of (II) is similar to the one used in the case of \mathbb{Z} in the main result of [2].

3. ON THE PROBABILITY OF A TOTALLY RAMIFIED EXTENSION OF GLOBAL FUNCTION FIELDS

In this section we are interested in obtaining the “probability” that a random extension of a given function field is totally ramified in a good way at some place. If F/\mathbb{F}_q is a function field with full constant field \mathbb{F}_q and E is a finite extension of F , we recall that an extension of places $Q|P$ is said to be *totally ramified* if the dimension of \mathcal{O}_Q/Q as an \mathcal{O}_P/P vector space is equal to 1.

The notion of “good” total ramification is encoded in the following

Definition 3.1. Let $E : F$ be a separable totally ramified extension of function fields. We say that $E : F$ is *nicely totally ramified with respect to* $f(T) \in F[T]$ if

- $f(X)$ is the defining polynomial of E , i.e. $E \cong F[y]/(f(y))$.
- there exists a totally ramified extension of places $Q \mid P$ of $E : F$ such that $\mathcal{O}_P[y] = \mathcal{O}_Q$.

The reader with some insight in algebraic geometry can read the condition of nice total ramification as a condition of “non-singularity” around the totally ramified place.

Our purpose is now to compute the density of degree n polynomials $f(X)$ of $F[X]$ for which $f(X)$ is irreducible and the extension $F[y]/(f(y)) : F$ is nicely totally ramified with respect to $f(X)$.

3.1. A characterization of polynomials defining nice totally ramified extensions. First of all, we convert the nice total ramification property into properties of the coefficients of the defining polynomials. Let us start by stating some well known facts on totally ramified extensions.

Lemma 3.2. *Let $Q \mid P$ be an extension of places of the function field extension $E : F$. Let u be a uniformizer for Q , $E = F(u)$ and f_u be the minimal polynomial for u over \mathcal{O}_P . Then*

- if $Q \mid P$ is totally ramified, we have that $\mathcal{O}_P[u] = \mathcal{O}_Q$;
- f_u is an Eisenstein polynomial if and only if $Q \mid P$ is totally ramified.

Proof. To see this, simply combine [13, Proposition 3.1.15] and [13, Proposition 3.5.12]. \square

Proposition 3.3. *Let k be a perfect field and f be an irreducible separable polynomial of degree $n \geq 2$ over a function field F/k . Let $E = F[y]/(f(y))$ and $Q \mid P$ be a totally ramified extension of places of $E : F$. Then we have*

- (i) *if y is holomorphic at Q , then $\mathcal{O}_P[y] = \mathcal{O}_Q$ if and only if $f(T + u)$ is an Eisenstein polynomial for some u in \mathcal{O}_P .*
- (ii) *if y is not holomorphic at Q , then $\mathcal{O}_P[1/y] = \mathcal{O}_Q$ if and only if $T^n f(1/T)$ is Eisenstein.*

Proof. Let us prove (i). Suppose $\mathcal{O}_P[y] = \mathcal{O}_Q$, then there exists $u \in \mathcal{O}_P$ such that $y(Q) = u(Q) = u(P)$. Let $z = y - u$. The minimal polynomial of z is $f(T + u)$, which implies that if we can prove that $v_Q(z) = 1$, it will follow that $f(T + u)$ is Eisenstein

with respect to P . It is easily seen that $\mathcal{O}_P[y] = \mathcal{O}_P[z] = \mathcal{O}_Q$, therefore if x is a uniformizer for Q , we can write

$$x = \sum_{i=0}^{n-1} a_i z^i$$

for some $a_i \in \mathcal{O}_P$. Whence,

$$1 = v_Q \left(\sum_{i=0}^{n-1} a_i z^i \right) \geq \min_{i \in \{0, \dots, n-1\}} \{v_Q(a_i) + i v_Q(z)\}.$$

Since $x(Q) = z(Q) = 0$, we get $v_Q(a_0) = n v_Q(a_0) \geq n > 1$, which forces $v_Q(z) = 1$, as $n \geq 2$.

Now suppose that $f(T + u)$ is Eisenstein with respect to some P . It follows that $z = y - u$ is a uniformizer for Q , which implies $\mathcal{O}_P[y] = \mathcal{O}_P[z] = \mathcal{O}_Q$.

The claim (ii) easily follows by applying (i) to $\bar{y} = 1/y$ with $u = 0$. \square

The following corollary shows that the polynomials which are Eisenstein after a Moebius transformation are not more than the ones which are Eisenstein after either a shift or an inversion. This result is not needed in the proof of the main theorem, nevertheless we include it for completeness (in the case of \mathbb{Z} , this question was asked in [14]).

Corollary 3.4. *Let f be a polynomial of degree $n \geq 2$ and P a place of F . The following are equivalent:*

- (i) *There exist $h, s, l, j \in \mathcal{O}_P$ such that $hj - sl \in \mathcal{O}_P^*$ and $g(T) = (lT + j)^n f(\frac{hT+s}{lT+j})$ is Eisenstein;*
- (ii) *One of the following two occurs:*
 - *$f(T + u)$ is Eisenstein with respect to P for some $u \in \mathcal{O}_P$.*
 - *$T^n f(1/T)$ is Eisenstein with respect to P .*

Proof. Clearly (ii) implies (i). Let us now prove that (ii) follows from (i). Let $m'(T) = \frac{aT+b}{cT+d}$ be the inverse of $m(T) = \frac{hT+s}{lT+j}$. Suppose y is a zero of $f(T)$ and is holomorphic at the totally ramified place $Q \subseteq F(y)$ lying over P . The element $\tilde{y} := \frac{ay+b}{cy+d}$ is then a zero of the Eisenstein polynomial $g(T)$ therefore by 3.2 and the fact that $F(y) = F(\tilde{y})$ we have that $\mathcal{O}_P[\tilde{y}] = \mathcal{O}_Q$. Suppose y is holomorphic at P , then it is enough to show that $\mathcal{O}_P[y] = \mathcal{O}_P[m(\tilde{y})] = \mathcal{O}_Q$. To this end, we observe that

$$y(Q) = \frac{h(Q)\tilde{y}(Q) + s(Q)}{l(Q)\tilde{y}(Q) + j(Q)} = \frac{s(Q)}{j(Q)}.$$

By the above equation it follows that the element

$$(3.1) \quad z = y - s/j = \frac{hj - sl}{j(l\tilde{y} + s)}\tilde{y}$$

has valuation greater than 1 at Q and $v_P(hj - sl) = 0$ as $v_P(ad - bc) = 0$. As y is holomorphic at Q , we have that $j(Q) \neq 0$ since

- if $s(Q) \neq 0$, then $j(Q) \neq 0$ since $y(Q) = s(Q)/j(Q)$
- suppose that $s(Q) = 0$, then $j(Q)$ cannot be zero as $h(Q)j(Q) - s(Q)l(Q) \neq 0$.

If we can show that z has valuation 1 we are done, as we would have by (3.1)

$$\mathcal{O}_Q = \mathcal{O}_P[z] = \mathcal{O}_P[y].$$

Since $v_Q(j) = 0$, we have

$$1 \leq v_Q(z) = 1 - v_Q(l\tilde{y} + s) \leq 1$$

which concludes the proof in the case in which y is holomorphic at Q . If y is not holomorphic at Q , we choose \tilde{y} as before and $t = 1/y$. Now it holds $t = \frac{l\tilde{y} + s}{h\tilde{y} + s}$ and the previous considerations can be applied again to show $\mathcal{O}_P[t] = \mathcal{O}_Q$. \square

3.2. On the density of totally ramified extensions of fixed degree. The following lemma gives the exact restriction for the set of possible shifts which are candidates for turning a given polynomial $f(X)$ into an Eisenstein polynomial.

Lemma 3.5. *Let \mathcal{O}_P be a valuation ring of a function field F and let $f \in \mathcal{O}_P[T]$ of degree $d = \deg(f) \geq 2$. Let $G_P \subseteq \mathcal{O}_P$ be a set of representatives of \mathcal{O}_P/P . We have that $f(T + i)$ is Eisenstein with respect to P for some $i \in \mathcal{O}_P$ if and only if $f(T + i)$ is Eisenstein with respect to P for some $i \in G_P$.*

Proof. One implication is obvious so let us prove the other direction. Suppose that $f(T) = \sum_{i=0}^d a_i T^i$ for $a_i \in \mathcal{O}_P$ and that $f(T + i)$ is P -Eisenstein for some $i \in \mathcal{O}_P$. Let us first show that, for any $p \in P$, the polynomial $f(T + p)$ is Eisenstein if and only if $f(T)$ is Eisenstein. This follows by the fact that the conditions modulo P of f are easily verified as $f(T + p) = f(T) \pmod{P}$. The condition modulo P^2 reduces to check that $f(p) \neq 0 \pmod{P^2}$, which indeed holds as $f(p) = \sum_{i=0}^d a_i p^i = a_0 \neq 0 \pmod{P}$. The proof is now straightforward, since any $i \in \mathcal{O}_P$ can be written as $j + p$ for some $j \in G_P$ and $p \in P$: we have that $f(T + i) = f(T + j + p)$ is P -Eisenstein and then $f(T + j)$ is P -Eisenstein for $j \in G_P$. \square

We are now ready to extract the density of the set the set of polynomials in question using the local to global principle together with some tools from measure theory and linear algebra. With a small abuse of notation, in what follow we will identify with \mathbb{H}^{n+1} the set of degree n polynomials over a holomorphy ring \mathbb{H} .

Theorem 3.6. *Let $\mathbb{H}_{\mathcal{S}}$ be a holomorphy ring of a global function field F/\mathbb{F}_q having full constant field \mathbb{F}_q . The set of polynomials $f \in \mathbb{H}[T]$ of degree $n \geq 3$ such that the ring $E = F[y]/(f(y))$ is a field and $E : F$ is nicely totally ramified with respect to f , has density*

$$R(n, \mathbb{H}) = 1 - \prod_{P \in \mathcal{S}} \frac{(q^{\deg(P)} - 1)^2 (q^{\deg(P)} + 1)}{q^{\deg(P)(n+2)}}.$$

Proof. First, we should observe that we can restrict to the separable case, as the set of inseparable polynomials has density zero. Let us denote the complement of \mathcal{S} in \mathbb{P}_F by \mathcal{S}^c . First, we should prove that if ramification occurs, it occurs with probability one at a place of \mathcal{S} . In fact, the polynomials $f(T) \in \mathbb{H}_{\mathcal{S}}[T]$ defining a totally ramified extension $E : F$ at a place of \mathcal{S}^c , do not contribute to $R(n, \mathbb{H})$. This is not surprising, as the definition of the density depends on the choice of \mathcal{S} . In particular we prove:

Claim 1. *The density of degree n polynomials in $\mathbb{H}_{\mathcal{S}}[T]$ for which $E : F$ is nicely totally ramified equals the density of degree n polynomials in $\mathbb{H}_{\mathcal{S}}[T]$ for which $E : F$ is nicely totally ramified at a place of \mathcal{S} .*

Proof of Claim 1.

Let

$$A := \{f \in \mathbb{H}_{\mathcal{S}}[T] : f \text{ is Eisenstein for some shift } i \in G_P \text{ and some place } P \in \mathcal{S}^c\}$$

and

$$B = \{f \in \mathbb{H}_{\mathcal{S}}[T] : T^n f(1/T) \text{ is Eisenstein for some place } P \in \mathcal{S}^c\}$$

It is enough to show that $C = A \cup B$ has density zero. First, we show that if $f \in C$, then $f \in \mathcal{O}_P[T]$ for some $P \in \mathcal{S}^c$. Clearly, if $f \in B$ this follows immediately by the definition of Eisenstein polynomial. Let now suppose that $f \in A$. Let $f = \sum_{j=0}^n a_j T^j$ and $i \in G_P$ such that $f(T+i) = \sum_{j=0}^n b_j T^j$ is Eisenstein. It is necessary now to observe that the map defined by the shift $\sigma_i : F^{n+1} \rightarrow F^{n+1}$ defined by $\sigma_i(f) = f(T+i)$ is linear, upper triangular in the basis $\{1, \dots, T^n\}$, and any element on the diagonal is 1. This shows recursively that if $a_j \in \mathcal{O}_P$ for all $j \in \{\ell+1, \dots, n\}$, then $a_\ell \in \mathcal{O}_P$. This is enough to conclude, since $a_n = b_n \in \mathcal{O}_P$.

Thanks to what we just proved, it is now clear that $C \subseteq \bigcup_{P \in \mathcal{S}^c} \mathbb{H}_{\mathcal{S} \cup P}^{n+1}$. Since the complement of \mathcal{S} is finite, we have that

$$\overline{\mathbb{D}}_{\mathcal{S}}(C) \leq \sum_{P \in \mathcal{S}^c} \overline{\mathbb{D}}_{\mathcal{S}}(\mathbb{H}_{\mathcal{S} \cup P}^{n+1}).$$

It follows that if we can show $\overline{\mathbb{D}}_{\mathcal{S}}(\mathbb{H}_{\mathcal{S} \cup P}^{n+1}) = 0$ we are done. To see this, let us consider for $D \in \mathcal{D}_{\mathcal{S}}$ the quantity $Q(D, P) := |\mathcal{L}(D) \cap \mathbb{H}_{\mathcal{S} \cup P}|$. For a divisor $D \in \mathcal{D}_{\mathcal{S}}$ of large degree, $Q(D, P)$ is easy to estimate, as one can write $D = D' + mP$ with $P \notin \text{supp}(D')$ and m positive integer. Then $Q(D, P) = Q(D', P) = q^{\deg(D') + 1 - g}$. It follows that

$$\frac{|Q(D, P)|}{q^{\ell(D' + mP)}} = \frac{|Q(D', P)|}{q^{\ell(D' + mP)}} \leq Cq^{-m \deg(P)}$$

which concludes the proof, as

$$\overline{\mathbb{D}}_{\mathcal{S}}(\mathbb{H}_{\mathcal{S} \cup P}) = \limsup_{D \rightarrow \infty} \frac{|Q(D, P)|^{n+1}}{q^{(n+1)\ell(D)}}.$$

End of the proof of Claim 1

From now on in this proof \mathcal{S} will be fixed, therefore we will denote $\mathbb{H}_{\mathcal{S}}$ and $\mathbb{D}_{\mathcal{S}}$ by \mathbb{H} and \mathbb{D} respectively. For any $P \in \mathcal{S}$, let $\hat{\mathcal{O}}_P$ be the P -adic completion of \mathcal{O}_P . With a small abuse of notation, let us identify with $\hat{\mathcal{O}}_P^{n+1}$ the set of polynomials of degree n in $\hat{\mathcal{O}}_P[T]$. Let now G_P be a set of representatives of the elements $\hat{\mathcal{O}}_P/P$. For any $a \in G_P$ we define the linear maps

$$\sigma_a : \hat{\mathcal{O}}_P^{n+1} \longrightarrow \hat{\mathcal{O}}_P^{n+1}$$

$$p(T) \mapsto p(T + a)$$

and

$$\text{inv} : \hat{\mathcal{O}}_P^{n+1} \longrightarrow \hat{\mathcal{O}}_P^{n+1}$$

$$p(T) \mapsto T^n p\left(\frac{1}{T}\right).$$

Let V_P be the set of Eisenstein polynomial of degree n over $\hat{\mathcal{O}}_P$ i.e.

$$V_P = \underbrace{(P\hat{\mathcal{O}}_P \setminus P^2\hat{\mathcal{O}}_P) \times P\hat{\mathcal{O}}_P \times \cdots \times P\hat{\mathcal{O}}_P \times (\hat{\mathcal{O}}_P \setminus P\hat{\mathcal{O}}_P)}_{n+1}.$$

We want now to compute the measure of the set of degree n polynomials which are Eisenstein after some shift or inversion.

Claim 2. *The P -measure of $U_P := (\bigcup_{a \in G_P} \sigma_a(V_P)) \cup \text{inv}(V_P)$ is*

$$\mu_P(U_P) = q^{-\deg(P)(n-1)}(1 - q^{\deg(P)})^2(q^{\deg(P)} + 1).$$

Proof of Claim 2.

We first want to show that the union above is disjoint. First, let us show that for any $a \neq 0$ in G_P we have $\sigma_a(V_P) \cap V_P = \emptyset$. This is easy, since for $g(T) \in \sigma_a(V_P) \cap V_P$, we have that the degree zero coefficient of $g_a(T) = g(T + a)$ is $g(a)$ and $g(T) \in V_P$ which implies that it can be written as $g(T) = bT^n + p h(T)$ for $p \in P$, $b \in \mathcal{O}_P \setminus P$: it follows that $g(a) \notin P$. As an easy consequence of the previous fact, we have that $\sigma_a(V_P) \cap \sigma_{a'}(V_P) = \emptyset$ for $a, a' \in G_P$ and $a \neq a'$. In addition, the intersection of $\text{inv}(V_P)$ with any of the $\sigma_a(V_P)$ is also empty. To see this, suppose that $g_a(T) \in \text{inv}(V_P)$. The fact that the degree n coefficient of $g_a(T)$ is in $\mathcal{O}_P \setminus P$, is in contradiction with the fact that $g_a(T) \in \text{inv}(V_P)$. In order to get the final claim, it is enough to compute the measures of each one of the $\sigma_a(V_P)$ and of $\text{inv}(V_P)$. It is easy to see that the maps σ_a and inv are indeed F -linear maps with determinant one, therefore $\mu_P(\sigma_a(V_P)) = \mu_P(\text{inv}(V_P)) = \mu_P(V_P)$ for any $a \in G_P$. The problem is then reduced to computing $\mu_P(V_P)$. As V_P is diagonal, one can obtain the measures of each of its component and then compute the product in order to get the wanted result. These measures are indeed easy to compute

$$\begin{aligned}\mu_P(P\widehat{\mathcal{O}}_P) &= q^{-\deg(P)}, \\ \mu_P(P\widehat{\mathcal{O}}_P \setminus P^2\widehat{\mathcal{O}}_P) &= q^{-\deg(P)} - q^{-2\deg(P)},\end{aligned}$$

and

$$\mu_P(\widehat{\mathcal{O}}_P \setminus P\widehat{\mathcal{O}}_P) = 1 - q^{-\deg(P)}.$$

It follows that

$$\mu_P(U_P) = \mu_P(\text{inv}(V_P)) + \sum_{a \in G_P} \mu_P(V_P) = (1 + q^{\deg(P)})\mu_P(V_P)$$

End of the proof of Claim 2

Clearly, we have an embedding ι_P of \mathbb{H} into $\widehat{\mathcal{O}}_P$. Using this embedding and Proposition 3.3 we have that the polynomial $f \in \mathbb{H}[T]$ defines a nicely totally ramified extension of F at P if and only if $\iota_P(f) \in U_P$. In fact, if f defines a nicely totally ramified extension $E = F[y]/f(y)$ then we are in one of the two cases of Proposition 3.3, as either $\mathcal{O}_P[y] = \mathcal{O}_Q$ or $\mathcal{O}_P[1/y] = \mathcal{O}_Q$ for some $Q|P$ totally ramified, which implies that either $\iota_P(f) \in \sigma_a(V_P)$ for some $a \in G_P$ or $\iota_P(f) \in \text{inv}(V_P)$. Vice versa, suppose that $\iota_P(f) \in U_P$, then $f(T + a)$ is Eisenstein for some a or $T^n f(1/T)$ is Eisenstein. This implies that the extension $F[y]/(f(y))$ is totally ramified by Lemma 3.2, as $F(y + a) = F(1/y) = F(y)$. We have now to show that the total ramification is

nice. We observe that, if $Q|P$ is the totally ramified extension then \mathcal{O}_Q is the integral closure of \mathcal{O}_P by Lemma 3.2. Therefore, if $\iota_P(f) \in \sigma_a(V_P)$ for some $a \in G_P$, then y is holomorphic at Q , otherwise, if $\iota_P(f) \in \text{inv}(V_P)$, then $1/y$ is holomorphic at Q , from which it follows that we end up again in one of the cases of Proposition 3.3.

Claim 3. *Let t be a positive integer and \mathcal{S}_t be the set of places of \mathcal{S} of degree larger than t . We have*

$$\lim_{t \rightarrow \infty} \overline{\mathbb{D}}(\{a \in \mathbb{H}^{n+1} \mid a \in U_P \text{ for some } P \in \mathcal{S}_t\}) = 0.$$

Proof of Claim 3.

By recalling the definition of U_P we can split the limit above as $\lim_{t \rightarrow \infty} \overline{\mathbb{D}}(I_t) + \overline{\mathbb{D}}(A_t)$ where

$$I_t = \{a \in \mathbb{H}^{n+1} \mid a \in \text{inv}(V_P) \text{ for some } P \in \mathcal{S}_t\}$$

and

$$A_t = \{a \in \mathbb{H}^{n+1} \mid a \in \bigsqcup_{a \in G_P} \sigma_a(V_P) \text{ for some } P \in \mathcal{S}_t\}.$$

Let us first deal with the limit in I_t , which is the easy part. By recalling the definition of the linear operator inv , and by considering only the conditions on the coefficients of the terms of degree n and $n-1$, it is easy to observe that

$$I_t \subseteq \{(x_0, \dots, x_n) \in \mathcal{L}(D)^n \mid x_{n-1} \equiv x_n \equiv 0 \pmod{P} \text{ for some } P \in \mathcal{S}_t\} = I'_t.$$

As x_n and x_{n-1} are indeed coprime polynomials, $\lim_{t \rightarrow \infty} \overline{\mathbb{D}}(I_t) = \lim_{t \rightarrow \infty} \overline{\mathbb{D}}(I'_t) = 0$ by Theorem 2.2.

It remains to show that $\lim_{t \rightarrow \infty} \overline{\mathbb{D}}(A_t) = 0$. We now produce two equations associated to A_t via elementary elimination theory, the final claim will follow again by Theorem 2.2. Let us write a generic shift for a generic polynomial of degree n :

$$f(T) = \sum_{i=0}^n x_i T^i \in F[x_1, \dots, x_n, T]$$

$$f(T+z) = \sum_{i=0}^n c_i(x_i, \dots, x_n, z) T^i \in F[x_1, \dots, x_n, z, T],$$

for some polynomial functions $c_i(x_i, \dots, x_n, z) \in F[x_i, \dots, x_n, z]$. Notice that the polynomial c_i depends only on the last $n-i$ variables since the shift map is upper triangular. In particular, let (y_0, \dots, y_n) be a specialization to elements of \mathbb{H} such that the given polynomial $f(T) = \sum_{i=0}^n y_i T^i$ is in A_t . Then, there exists $\bar{z} \in \mathbb{H}$ such that $c_0(y_0, \dots, y_n, \bar{z}) \equiv c_1(y_1, \dots, y_n, \bar{z}) \equiv c_{n-1}(y_{n-1}, y_n, \bar{z}) \equiv 0 \pmod{P}$ for some

$P \in \mathcal{S}$. Let us now explicitly compute c_0, c_1 and c_{n-1} :

$$\begin{aligned} c_0(x_0, \dots, x_n, z) &= f(z) = \sum_{i=0}^n x_i z^i \\ c_1(x_1, \dots, x_n, z) &= f'(z) = \sum_{i=1}^n i x_i z^{i-1} \\ c_{n-1}(x_{n-1}, x_n, z) &= x_{n-1} - \tilde{n} x_n z, \end{aligned}$$

where we set $\tilde{n} = -n$ to simplify the computations that follow. Observe that c_{n-1} is distinct from c_1 as $n > 2$. Recall that we want to apply Theorem 2.2 so we have to eliminate the variable z , getting two equations. In order to do that, we have to distinguish two possibilities, depending on whether the characteristic of F divides n or not. In case n is divisible by $\text{Char}(F)$, then two polynomials which eliminate z are $\text{Res}_z(f(z), f'(z)) = \text{Disc}_z(f(z)) \in F[x_0, \dots, x_n]$ and x_{n-1} . Define $A'_t = \{f \in \mathbb{H}^{n+1} \mid \text{Disc}_z(f) \equiv x_{n-1} \equiv 0 \pmod{P} \text{ for some } P \in \mathcal{S}_t\}$. By Theorem 2.3 we get that $\lim_{t \rightarrow \infty} \overline{\mathbb{D}}(A'_t) = 0$. Observe that by construction $A_t \subseteq A'_t$, from which the claim follows.

It remains to deal with the case in which n is not divisible by $\text{Char}(F)$. We can eliminate the variable z from the ideal

$$\langle c_0(x_0, \dots, x_n, z), c_1(x_1, \dots, x_n, z), c_{n-1}(x_{n-1}, x_n, z) \rangle \subseteq F[x_0, \dots, x_n, z]$$

by multiplying c_0 by $(\tilde{n}x_n)^{n-1}$ and c_1 by $(\tilde{n}x_n)^{n-2}$ and using the relation given by c_{n-1} , getting two polynomials:

$$\begin{aligned} f_0(x_0, \dots, x_n) &:= x_{n-1}^n \tilde{n}^{-1} + \sum_{i=0}^{n-1} (\tilde{n}x_n)^{n-1-i} x_i x_{n-1}^i \\ f_1(x_1, \dots, x_n) &:= -x_{n-1}^{n-1} + \sum_{i=1}^{n-1} i (\tilde{n}x_n)^{n-2-(i-1)} x_i x_{n-1}^{i-1}. \end{aligned}$$

We define now $A'_t \supseteq A_t$ as the set of specializations $(y_0, \dots, y_n) \in \mathbb{H}^{n+1}$ such that $f_0(y_0, \dots, y_n) \equiv f_1(y_1, \dots, y_n) \equiv 0 \pmod{P}$ for some place P of degree larger than t . It remains to show that f_0 and f_1 are coprime, then we will get $\lim_{t \rightarrow \infty} \overline{\mathbb{D}}(A_t) \leq \lim_{t \rightarrow \infty} \overline{\mathbb{D}}(A'_t) = 0$ by Theorem 2.3. First, observe that $f_1 \neq 0$ as $c_1 \neq c_{n-1}$ (since $n > 2$). Notice that $f_0 = x_0 h_1(x_1, \dots, x_n) \tilde{n}^{n-1} + h_0(x_1, \dots, x_n)$ for some $h_0, h_1 \in \mathbb{H}[x_1, \dots, x_n]$. On the other hand, x_0 does not appear in f_1 , which implies that, if there is an irreducible common factor g of f_0 and f_1 , then it must divide both h_0 and h_1 . In our specific case case, $h_1(x_1, \dots, x_n) = \tilde{n}^{n-1} x_n^{n-1}$ which forces $g = x_n$ but this is impossible, as for example $f_1(x_0, \dots, x_{n-1}, 0) \neq 0$.

End of the proof of Claim 3

We are now able to conclude the proof using Theorem 2.1. Let R be the set of degree n polynomials giving rise to a nice totally ramified extension and let us consider R^c . By looking at the definition of the map π in the Theorem 2.1 and by recalling the choice of the U_P 's, we have that $R^c = \pi^{-1}(\{\emptyset\})$. Therefore, since Condition (2.1) of Theorem 2.1 is verified by the previous claim, we have that

$$\mathbb{D}(R^c) = \mathbb{D}(\pi^{-1}(\{\emptyset\})) = \nu(\{T\}) = \prod_{P \in \mathcal{S} \setminus T} (1 - \mu_P(U_P))$$

from which the claim follow by Claim 2 and the fact that $\mathbb{D}(R) = 1 - \mathbb{D}(R^c)$. \square

In the proof of the previous result the restriction $n > 2$ is crucial only for the proof of Claim 3. In the following remark we briefly adapt the above strategy to the case $n = 2$.

Remark 3.7. For the sake of completeness we should also deal with the case $n = 2$. Let R be the set of separable irreducible degree 2 polynomials $f \in \mathbb{H}[T]$ for which the extension $F[y]/(f(y))$ is nicely totally ramified. For this, let \mathcal{S}_t^c be the set of places of \mathcal{S} of degree at most t . For $P \in \mathcal{S}_t^c$, let U_P be defined as in the proof of Theorem 3.6 and for $P \in \mathcal{S}_t$ let $U_P = \emptyset$. For any fixed t , one easily observes that

$$E_t := \pi^{-1}(\{\emptyset\}) \supseteq R^c$$

therefore

$$(3.2) \quad \lim_{t \rightarrow \infty} \mathbb{D}(E_t) \geq \mathbb{D}(R^c).$$

Now, for any fixed $t \in \mathbb{N}$, Condition (2.1) is verified, since the set of U_P is finite. Using Theorem 2.1 as before one gets that the density of E_t is

$$\mathbb{D}(E_t) = \prod_{P \in \mathcal{S}_t^c} \frac{(q^{\deg(P)} - 1)^2 (q^{\deg(P)} + 1)}{q^{\deg(P)(4)}}$$

which is now a finite product. Letting t go to plus infinity, the sequence $\mathbb{D}(E_t)$ converges to zero, which forces $\mathbb{D}(R^c) = 0$ and so $\mathbb{D}(R) = 1$.

Remark 3.8. The reader should notice that the condition on the fact that the total ramification is good is of fundamental importance in the proof of the result: in fact, it allows the conversion given by Proposition 3.3. It would be of great interest to understand what happens to the final density result of Theorem 3.6 when the condition in Definition 3.1 is removed.

4. THE DENSITY OF RECTANGULAR UNIMODULAR MATRICES

Using the local to global principle, in this section we close the problem of computing the density of rectangular unimodular matrices with entries in an integrally closed subring of a global function field. As a special case of the main result, we also get the density of such matrices with entries the ring $\mathbb{F}_q[x]$. Such matrices are of deep interest in coding theory since they are one of the key ingredients to define a convolutional code. In that context a rectangular unimodular matrix is usually said to be *left prime*, see for example [7, pg 122] for a characterization of such condition.

Definition 4.1. Let k, m be positive integers such that $k < m$. Let M be a $k \times m$ matrix having entries in a commutative ring R . We say that M is *rectangular unimodular* if it can be extended with $m - k$ rows in R^n to an element of $GL_m(R)$.

The reader should notice that in the definition above we require the extension of M to be an automorphism of R^m as an R -module.

Problem 4.2. What is the density of rectangular unimodular matrices of $\mathbb{H}^{k \times m}$?

The problem was first addressed in [15] in the case of $\mathbb{H} = \mathbb{F}_q[x]$. Unfortunately, the proof in [15] is not correct as a priori there is no reason for the infinite sum in the proof of [15, Theorem 1] to commute with the superior limit. This was also observed in [10], where it is present a partial fix of the issue, in the case in which the number of columns are at least the double of the number of rows. In what follows we provide the complete solution of the problem using the tools we developed in the first section for the general case of holomorphy rings. In order to do this, we have to construct the p -adic system of subsets used in Theorem 2.1. This can be done using the following result proved in [16].

Theorem 4.3. Let R be a Dedekind domain. Let M be a $k \times m$ matrix with entries in R and I_M be the ideal generated by the determinants of the maximal minors of M . Then M is rectangular unimodular if and only if $I_M = R$.

We are now able to state and prove the main theorem

Theorem 4.4. Let F/\mathbb{F}_q be a function field with full constant field \mathbb{F}_q . Let \mathcal{S} be a set of places in \mathbb{P}_F having finite complement. The density of the set U of $k \times m$ rectangular unimodular matrices with entries in $\mathbb{H}_{\mathcal{S}}$ is

$$\mathbb{D}_{\mathcal{S}}(U) = \prod_{i=m-k+1}^m \frac{1}{\zeta_{\mathbb{H}}(i)},$$

where $\zeta_{\mathbb{H}}$ is the zeta function of \mathbb{H} defined as

$$\zeta_{\mathbb{H}}(s) = \zeta_F(s) \cdot \prod_{R \in \mathbb{P}_F \setminus \mathcal{S}} (1 - q^{-\deg(R)s}) = \prod_{P \in \mathcal{S}} (1 - q^{-\deg(P)s})^{-1}$$

and \mathcal{S} is the holomorphy set of \mathbb{H} .

Proof. For any $P \in \mathcal{S}$, let U_P be the set of non-unimodular matrices in $\widehat{\mathcal{O}}_P^{k \times m}$, i.e. the set of matrices for which the ideal generated by the determinant of the maximal minors is contained in $P\widehat{\mathcal{O}}_P$. By Theorem 4.3 we have that a matrix M is in U if and only if $M \notin U_P$ for any P . Therefore, in the notation of Theorem 2.1 it follows that $\pi^{-1}(\{\emptyset\}) = U$ and then, if the system $\{U_P\}$ verifies condition (2.1) we have that

$$\mathbb{D}_{\mathcal{S}}(U) = \prod_{P \in \mathcal{S}} (1 - \mu_P(U_P)).$$

In the polynomial ring

$$\mathbb{H}[x_{1,1}, x_{1,2}, \dots, x_{1,m}, x_{2,1}, \dots, x_{i,j}, \dots, x_{k,m}].$$

let us consider the $k \times m$ matrix whose i, j entry is the variable $x_{i,j}$. Let N, N' be two distinct $k \times k$ minors of this matrix and f and g be the determinants of N and N' respectively. Notice that f and g are distinct irreducible polynomials, therefore coprime. It is straightforward observe that the set $\{a \in \mathbb{H}_{\mathcal{S}}^d \mid a \in U_P \text{ for some } P \in \mathcal{S}_t\}$ is contained in $\{a \in \mathbb{H}_{\mathcal{S}}^d \mid f(a) \equiv g(a) \equiv 0 \pmod{P} \text{ for some } P \in \mathcal{S}_t\}$. By applying Theorem 2.3 one gets that the condition 2.1 is verified.

It remains to compute the P -measure of the U_P , the claim will follow by Proposition 3.3 and the fact that $\pi^{-1}(\{\emptyset\}) = U$. In order to compute such measures, we first decompose U_P . Let r be a representative in $\widehat{\mathcal{O}}_P^{k \times m}$ for a matrix in $(\mathcal{O}_P/P)^{k \times m}$ which is not full rank. We observe that the set $V_P(r) = \{M \in \mathcal{O}_P^{k \times m} : M = r + (P\widehat{\mathcal{O}}_P)^{k \times m}\}$ is contained in U_P . In addition, if $r, r' \in \mathcal{O}_P^{k \times m}$ and satisfy $r \not\equiv r' \pmod{P}$, then $V_P(r) \cap V_P(r') = \emptyset$. Let $R_P \subseteq \widehat{\mathcal{O}}_P$ be a set of representatives for the non-full rank matrices of $(\mathcal{O}_P/P)^{k \times m}$. Therefore, for fixed P the union of such $V_P(r)$ is disjoint and covers the whole U_P , from which it follows that

$$\mu_P(U_P) = \mu_P\left(\bigsqcup_{r \in R_P} V_P(r)\right) = \sum_{r \in R_P} \mu_P(V_P(r)).$$

Since

$$\mu_P(V_P(r)) = \mu_P(V_P(r) - r) = \mu_P(P\widehat{\mathcal{O}}_P)^{mk} = q^{-mk \deg(P)}$$

and the number of non-full rank matrices in $(\mathcal{O}_P/P)^{k \times m}$ is

$$q^{mk \deg(P)} - \prod_{i=0}^{k-1} \left(q^{\deg(P)m} - q^{\deg(P)i} \right),$$

one gets that

$$\mu_P(U_P) = 1 - q^{-mk \deg(P)} \prod_{i=0}^{k-1} \left(q^{\deg(P)m} - q^{\deg(P)i} \right) = 1 - \prod_{i=0}^{k-1} \left(1 - q^{-\deg(P)(m-i)} \right).$$

Therefore, by applying Theorem 2.1 we get $\mathbb{D}_{\mathcal{S}}(U) = \prod_{P \in \mathcal{S}} (1 - \mu_P(U_P))$. Exchanging now the finite product with the product over all the places, we get

$$\mathbb{D}_{\mathcal{S}}(U) = \prod_{i=0}^{k-1} \frac{1}{\zeta_{\mathbb{H}}(m-i)}$$

which is the result we wanted. \square

Remark 4.5. Notice that the density can be explicitly computed by the closed expression of the zeta function [13, Corollary 5.1.12, (b)] and the fact that $\mathbb{P}_F \setminus \mathcal{S}$ is finite. Observe that this is consistent with the result obtained for unimodular rows in the general case of global fields [11, 17].

As an immediate corollary we have

Corollary 4.6. *Let $k < m$ be positive integers. The density of the set U of $k \times m$ rectangular unimodular matrices (i.e. left prime matrices) with coefficients in $\mathbb{F}_q[x]$ is*

$$\mathbb{D}(U) = \prod_{i=m-k+1}^m \frac{q^{i-1} - 1}{q^{i-1}}.$$

Proof. Let $\mathbb{F}_q(x)$ be the rational function field and P_{∞} be the place at infinity of $\mathbb{F}_q(x)$. Recall that the zeta function of the rational function field is

$$\zeta_{\mathbb{F}_q(x)}(s) = \frac{1}{(1 - q^{-s})(1 - q^{-s+1})}.$$

Previously we already observed that

$$\mathbb{F}_q[x] = \bigcap_{P \neq P_{\infty}} \mathcal{O}_P$$

and therefore it follows that $\zeta_{\mathbb{F}_q[x]}(s) = 1/(1 - q^{-s+1})$. The claim follows by applying directly Theorem 4.4. \square

Remark 4.7. An analogous result in the case of \mathbb{Z} can be found in [18]. It would be of interest to use Theorem 2.1 to compute the density of matrices having fixed Smith Normal form, at least in the case in which the holomorphy ring is a PID (a result over \mathbb{Z} is already available in [19]).

ACKNOWLEDGEMENTS

We would like to thank Bjorn Poonen for very interesting discussions and for sharing his deep insight of the problem. We thank Elisa Gorla for suggesting a sophisticated modification of the proof of Theorem 2.2, which improved the paper in terms of length and clarity. We would like to also thank Federico Amadio, Francesca Balestrieri and Andrea Ferraguti for reading the preliminary version of this manuscript. This work started at MIT in Fall 2015 and was accomplished at the University of Oxford in Michaelmas 2016 under the Swiss National Science Foundation grant number 161757.

REFERENCES

- [1] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Annals of Mathematics*, 150(3):1109–1149, 1999.
- [2] Ekedahl Torsten. An infinite version of the chinese remainder theorem. *Commentarii mathematici Universitatis Sancti Pauli= Rikkyo Daigaku sugaku zasshi*, 40(1):53–59, 1991.
- [3] John L. Kelley. *General topology*. New York: Van Nostrand, 1955.
- [4] B. D. Sittinger. The probability that random algebraic integers are relatively r -prime. *Journal of Number Theory*, 130(1):164–171, 2010.
- [5] Andrei A Suslin. On projective modules over polynomial rings. *Sbornik: Mathematics*, 22(4):595–602, 1974.
- [6] Daniel Quillen. Projective modules over polynomial rings. *Inventiones Mathematicae*, 36(1):167–171, 1976.
- [7] Ettore Fornasini and Raquel Pinto. Matrix fraction descriptions in convolutional coding. *Linear Algebra and its Applications*, 392:119 – 158, 2004.
- [8] Joachim Rosenthal. Connections between linear systems and convolutional codes. In *Codes, Systems, and Graphical Models*, pages 39–66. Springer, 2001.
- [9] Xiangqian Guo and Guangyu Yang. The probability of rectangular unimodular matrices over $\mathbb{F}_q[x]$. *Linear Algebra and its Applications*, 438(6):2675–2682, 2013.
- [10] Giacomo Micheli and Reto Schnyder. The density of unimodular matrices over integrally closed subrings of function fields. In *Contemporary Developments in Finite Fields and Applications*, pages 244–253. World Scientific, 2016.

- [11] Giacomo Micheli and Reto Schnyder. On the density of coprime m -tuples over holomorphy rings. *International Journal of Number Theory*, 12(03):833–839, 2016.
- [12] Bjorn Poonen and Michael Stoll. A local-global principle for densities. In Scott D. Ahlgren, George E. Andrews, and K. Ono, editors, *Topics in Number Theory*, volume 467 of *Mathematics and Its Applications*, pages 241–244. Springer US, 1999.
- [13] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer, 2009.
- [14] Randell Heyman and Igor E. Shparlinski. On shifted Eisenstein polynomials. *Periodica Mathematica Hungarica*, 69(2):170–181, 2014.
- [15] Xiangqian Guo and Guangyu Yang. The probability of rectangular unimodular matrices over $F_q[x]$. *Linear Algebra and its Applications*, 438(6):2675–2682, 2013.
- [16] William H Gustafson, Marion E Moore, and Irving Reiner. Matrix completions over dedekind rings. *Linear and Multilinear Algebra*, 10(2):141–144, 1981.
- [17] Andrea Ferraguti and Giacomo Micheli. On the mertens–cesaro theorem for number fields. *Bulletin of the Australian Mathematical Society*, 93(02):199–210, 2016.
- [18] Gérard Maze, Joachim Rosenthal, and Urs Wagner. Natural density of rectangular unimodular integer matrices. *Linear Algebra and its Applications*, 434(5):1319–1324, 2011.
- [19] Yinghui Wang and Richard P Stanley. The smith normal form distribution of a random integer matrix. *arXiv preprint arXiv:1506.00160*, 2015.

MATHEMATICAL INSTITUTE, UNIVERSITY OF OXFORD, ANDREW WILES BUILDING, WOODSTOCK ROAD, OXFORD, UK

E-mail address: giacomo.micheli@ox.ac.uk